LIBYAN ACADEMY FOR TELECOM AND INFORMATICS

SECURITY + SY601 COURSE MODULE5

Instructor Khaled Gamo

Module5 Governance, Risk, and Compliance

Security Controls

his chapter covers CompTIA Security+ exam objective 5.1: Compare and contrast various types of controls.

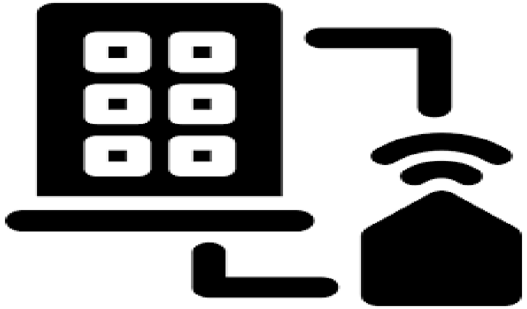
Security controls are the mechanisms employed to minimize exposure to risk and mitigate the effects of loss. Using the security attributes of confidentiality, integrity, and availability (CIA).

Security Controls

Categories of Security control

Managerial Administrative

Operational



Technical

Security Controls

Control Types

Preventative Controls

Examples of preventative controls include:

- Hardening
- Security Awareness Training
- Security Guards
- Change Management
- Account Disablement Policy

Detective Controls

Examples of detective controls include:

- Log Monitoring
- Trend Analysis
- Security Audits
- Video Surveillance
- Motion Detection

Security Controls

Control Types

Deterrent Controls

Deterrent controls reduce the likelihood of a deliberate attack and is usually in the form of a tangible object or person

Example of deterrent controls include:
Cable Locks
Hardware Locks
Video surveillance & guards

Compensating Controls

Examples of compensating controls include:

Time-based One Time-Password (TOTP) – A temporary passcode generated by an algorithm that uses the current time of day as one of its authentication factors.
Encryption – Database security applications, e-mail encryption and other tools.

Physical Controls

A physical control is one that prevents specific physical actions from occurring, such as a mantrap prevents tailgating. Physical controls prevent specific human interaction with a system and are primarily designed to prevent accidental operation of something.

Regulations, Standards, and Frameworks

Regulations, Standards, and Frameworks

his chapter covers CompTIA Security+ exam objective 5.2: Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.

Regulations, Standards, and Legislation

Business operations never happen in a vacuum; there are at least some policies and procedures one must follow. But these policies and procedures get their direction from regulations, standards, and legislation. Laws are made by the legislative bodies of government to create a specified set of conditions and penalties

Regulations, Standards, and Frameworks

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), which was a sweeping rewrite of European privacy regulations, went into effect in May of 2018.

The GDPR requires significant consideration, including the following:

- Assess personal data flows from the EU to the U.S. to define the scale and scope of the cross-border privacy-compliance challenge.
- Assess readiness to meet model clauses, remediate gaps, and organize audit artifacts of compliance with the clauses.
- Update privacy programs to ensure they are capable of passing an EU regulator audit.
- Conduct EU data-breach notification stress tests.
- Monitor changes in EU support for model contracts and binding corporate rules

Regulations, Standards, and Frameworks

National, Territory, or State Laws

Laws are the system of rules, or statutes, made by the government of a country, state, or city. Statutes are enacted by a legislative body and then signed by the ranking official (president/governor). With respect to cybersecurity, there are a wide variety of laws from the national and state levels.

Regulations, Standards, and Frameworks

Regulations, Standards, and Frameworks

Key Frameworks

Payment Card Industry Data Security Standard (PCI DSS)

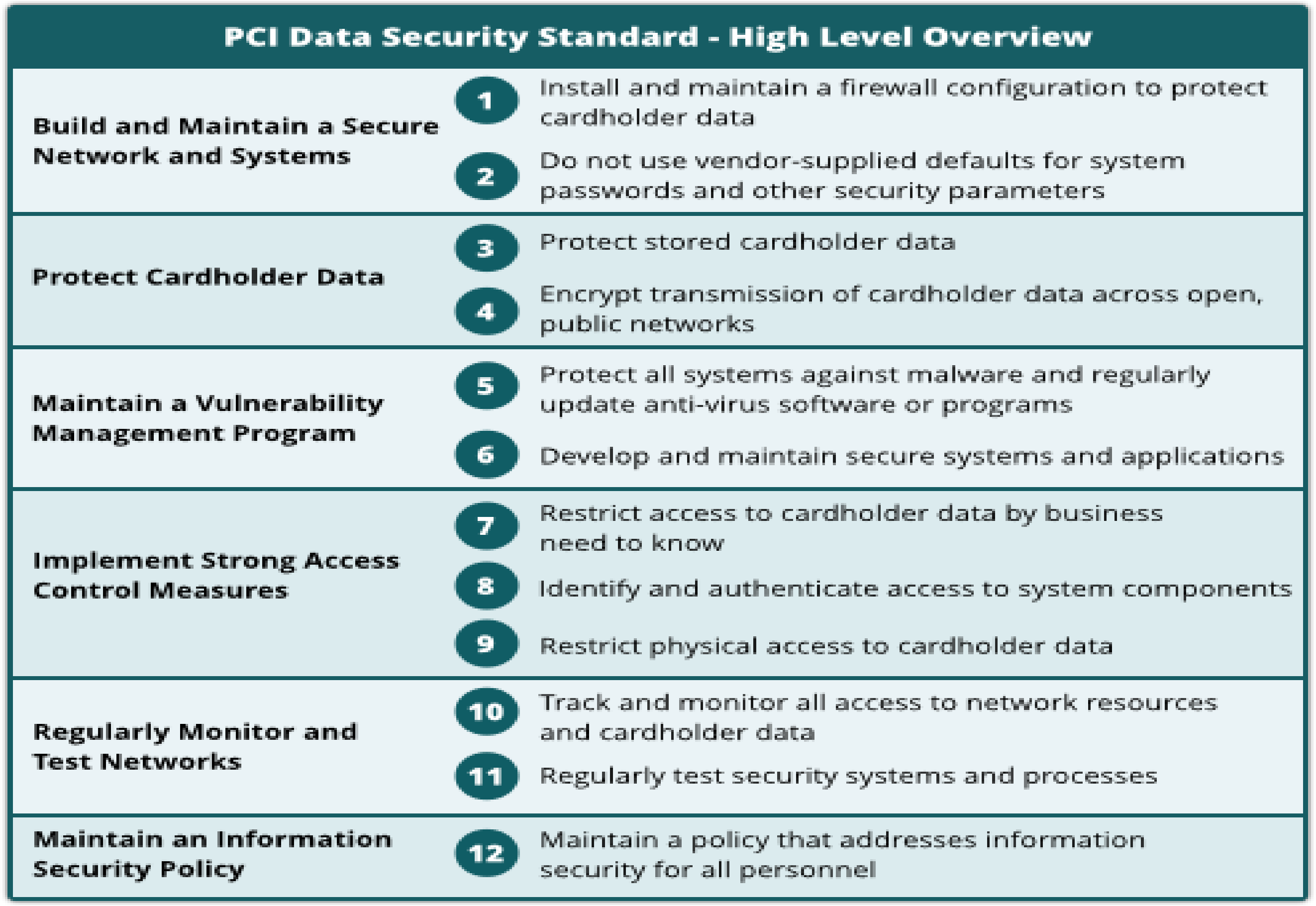
The payment card industry, including the powerhouses of MasterCard and Visa, through its PCI Security Standards Council, designed a private sector initiative to protect payment card information between banks and merchants. The Payment Card Industry Data Security Standard (PCI DSS) is a set of contractual rules governing how credit card data is to be protected

Regulations, Standards, and Frameworks

Key Frameworks

PCI DSS Objectives and Requirements

PCI DSS v3 includes six control objectives containing a total of 12 requirements:



PCI Data Security Standard - High Level Overview

Build and Maintain a Secure Network and Systems	1	Install and maintain a firewall configuration to protect cardholder data
	2	Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3	Protect stored cardholder data
	4	Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5	Protect all systems against malware and regularly update anti-virus software or programs
	6	Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7	Restrict access to cardholder data by business need to know
	8	Identify and authenticate access to system components
	9	Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10	Track and monitor all access to network resources and cardholder data
	11	Regularly test security systems and processes
Maintain an Information Security Policy	12	Maintain a policy that addresses information security for all personnel

Regulations, Standards, and Frameworks

Key Frameworks

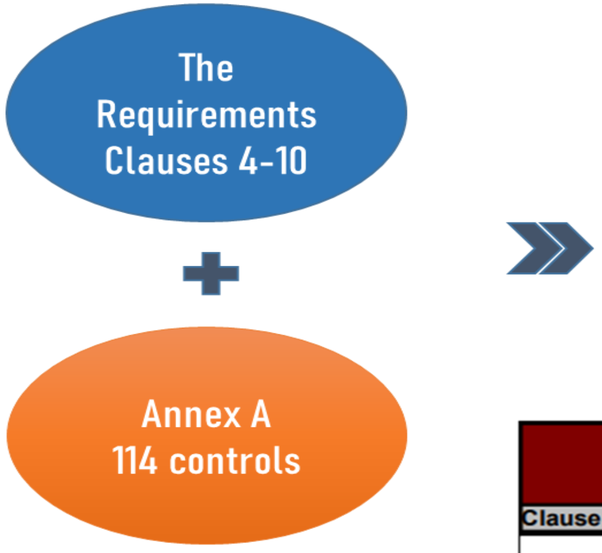
International Organization for Standardization (ISO) 27001/27002/27701/31000

- ISMS (Information Security Management System)
- Coordinated set of activities, processes, people and controls aimed at the protection and management of information
- An ISMS is not about technical security alone
- It is a management system!

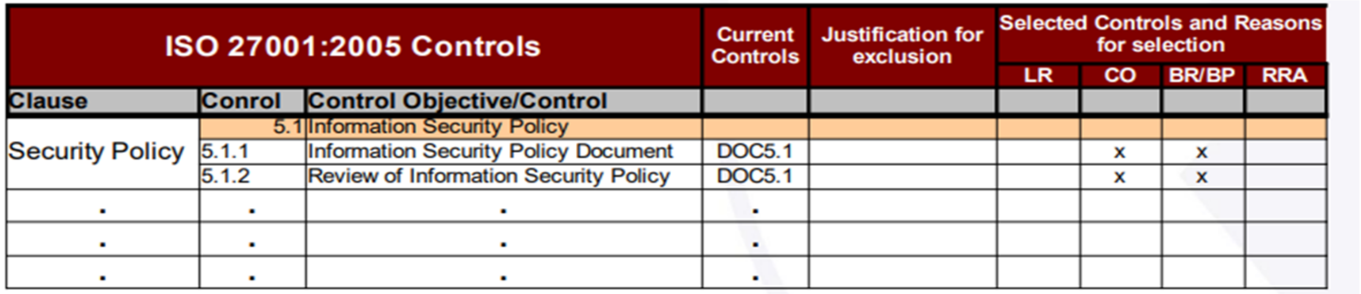
Regulations, Standards, and Frameworks

Key Frameworks

ISO/IEC 27001:2013



Key Requirement
Risk Management



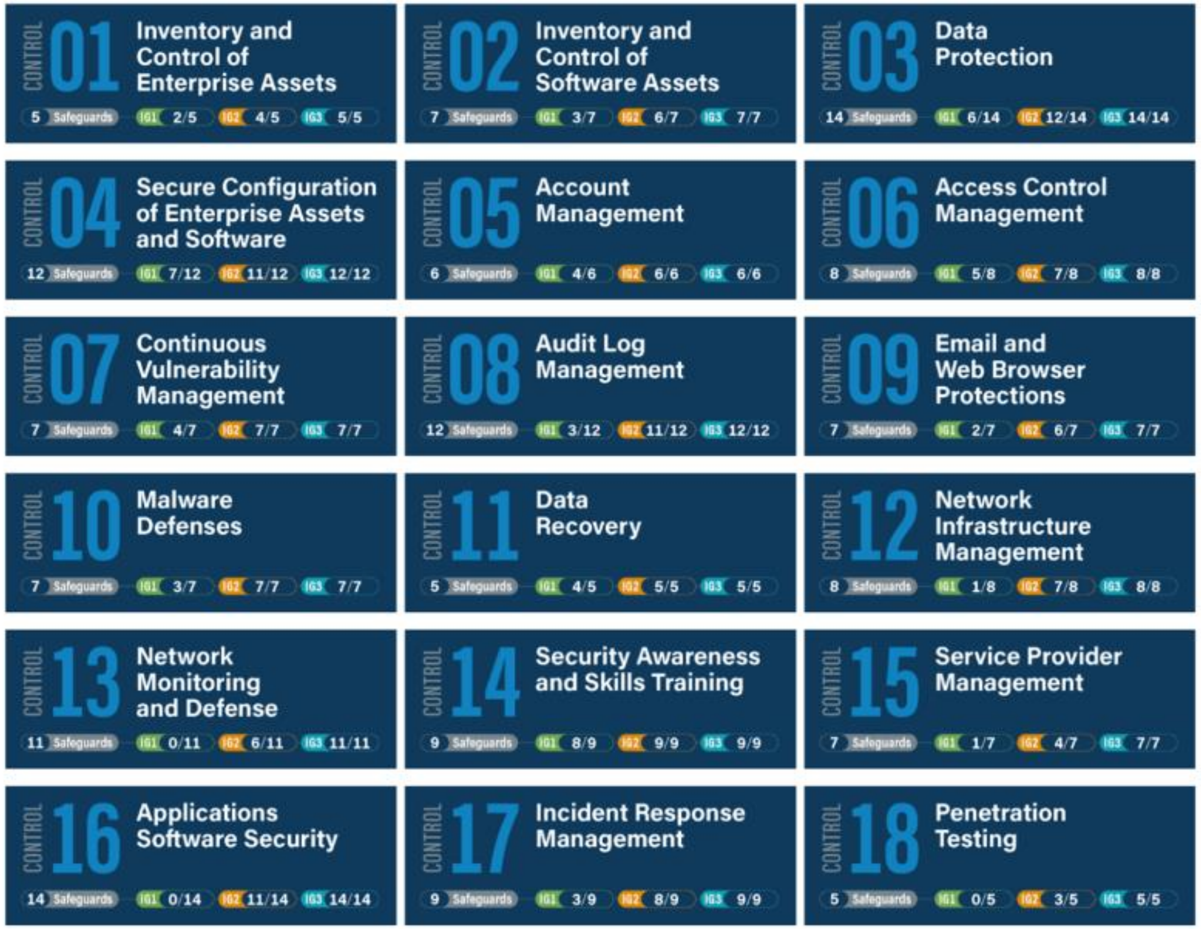
ISO 27001:2005 Controls			Current Controls	Justification for exclusion	Selected Controls and Reasons for selection			
					LR	CO	BR/BP	RRA
Clause	Conrol	Control Objective/Control						
Security Policy	5.1	Information Security Policy						
	5.1.1	Information Security Policy Document	DOC5.1			x	x	
	5.1.2	Review of Information Security Policy	DOC5.1			x	x	
.	.	.	.					
.	.	.	.					
.	.	.	.					

Regulations, Standards, and Frameworks

Key Frameworks

Center for Internet Security (CIS)

The Center for Internet Security (CIS) is a nonprofit organization that serves the cybersecurity community in a number of ways. It is the guardian of the CIS controls—a set of the top 20 security controls that should be implemented as a baseline of cybersecurity risk management.



CONTROL 01 Inventory and Control of Enterprise Assets
5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 02 Inventory and Control of Software Assets
7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 03 Data Protection
14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 04 Secure Configuration of Enterprise Assets and Software
12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 05 Account Management
6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 06 Access Control Management
8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 07 Continuous Vulnerability Management
7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 08 Audit Log Management
12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 09 Email and Web Browser Protections
7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10 Malware Defenses
7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11 Data Recovery
5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12 Network Infrastructure Management
8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13 Network Monitoring and Defense
11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14 Security Awareness and Skills Training
9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15 Service Provider Management
7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7

CONTROL 16 Applications Software Security
14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17 Incident Response Management
9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9

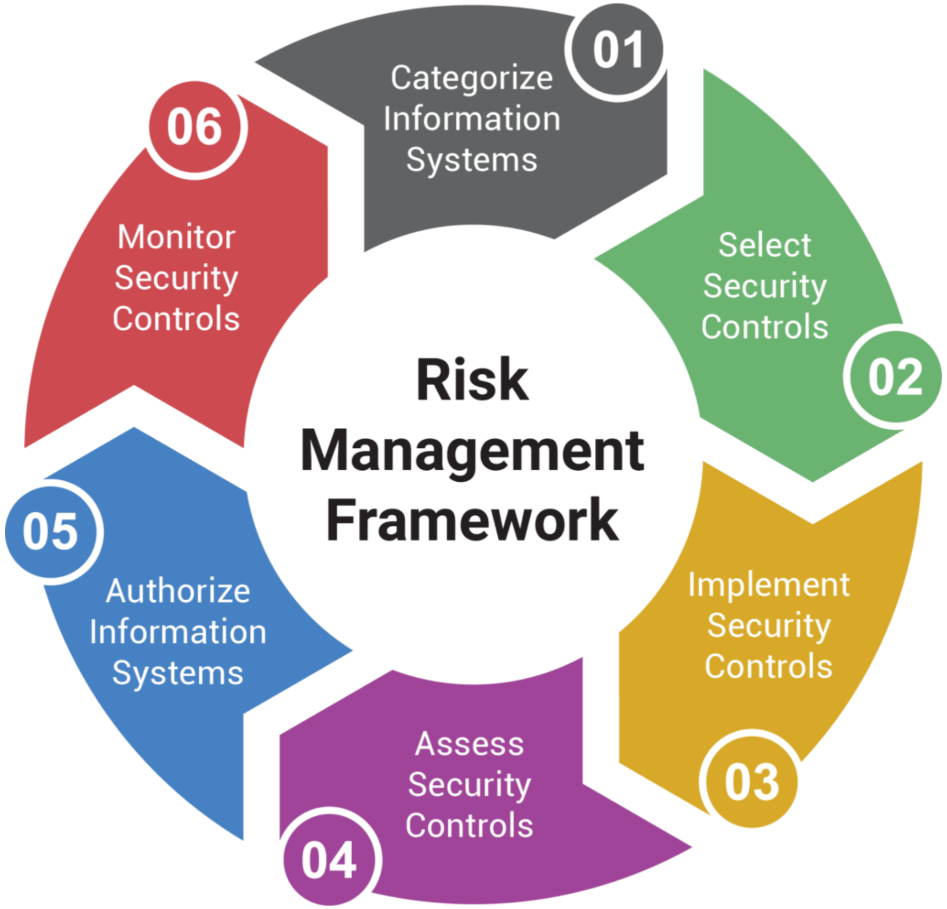
CONTROL 18 Penetration Testing
5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5

Regulations, Standards, and Frameworks

Key Frameworks

National Institute of Standards and Technology (NIST) Risk Management Framework

The National Institute of Standards and Technology (NIST) provides recommended strategies to the U.S. government and others on how to handle a wide range of issues, including risk from cybersecurity issues. The approach taken by NIST is one built around the management of organizational risk through a risk management framework (RMF) associated with cybersecurity activities. The NIST RMF is composed of more than 10 publications, spanning virtually every activity associated with cybersecurity.

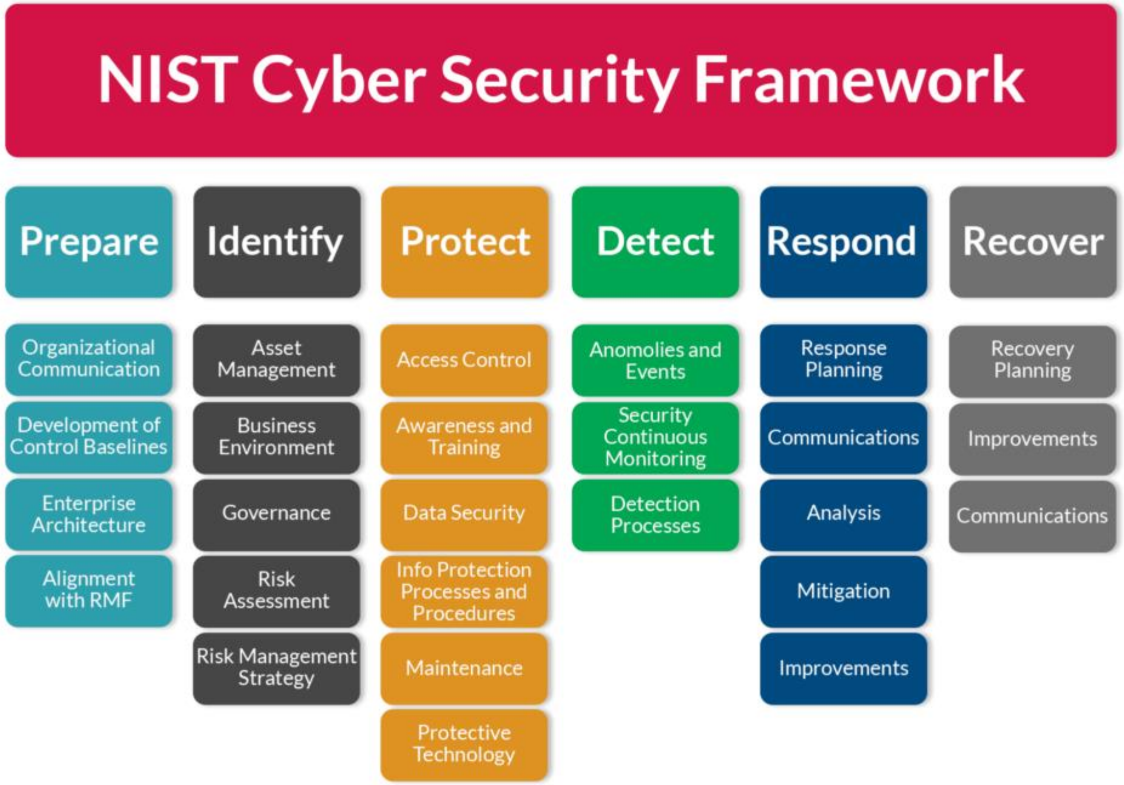

Risk Management Framework
01
Categorize Information Systems
02
Select Security Controls
03
Implement Security Controls
04
Assess Security Controls
05
Authorize Information Systems
06
Monitor Security Controls

Regulations, Standards, and Frameworks

Key Frameworks

National Institute of Standards and Technology (NIST) Risk Management Framework

A second activity published by NIST is the Cybersecurity Framework (CSF). The CSF is designed to assist organizations in the early stages of planning their cybersecurity posture. It breaks down the types of activities into five different functions: identify, protect, detect, respond, and recover.



NIST Cyber Security Framework

Prepare	Identify	Protect	Detect	Respond	Recover
Organizational Communication	Asset Management	Access Control	Anomolies and Events	Response Planning	Recovery Planning
Development of Control Baselines	Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Enterprise Architecture	Governance	Data Security	Detection Processes	Analysis	Communications
Alignment with RMF	Risk Assessment	Info Protection Processes and Procedures		Mitigation	
	Risk Management Strategy	Maintenance		Improvements	
		Protective Technology			

Regulations, Standards, and Frameworks

Key Frameworks

SSAE SOC 2 Type I/II

Statement on Standards for Attestation Engagements (SSAE) is a set of auditing standards set by the American Institute of Certified Public Accountants (AICPA) Auditing Standards Board. SOC stands for Service Organization Controls. An SOC 2 report focuses on the internal controls at an organization related to compliance or operations, wrapped around the five trust principles (security, confidentiality, processing integrity, availability, and privacy).

SOC 2 is a separate report that focuses on controls at a service provider relevant to security, availability, processing integrity, confidentiality, and privacy of a system. It ensures that your data is kept private and secure while in storage and in transit and that it is available for you to access at any time. The SOC 1 and SOC 2 reports come in two forms: Type I and Type II. Type I reports evaluate whether proper controls are in place at a specific point in time. Type II reports are done over a period of time to verify operational efficiency and effectiveness of the controls

Regulations, Standards, and Frameworks

Key Frameworks

Cloud Security Alliance

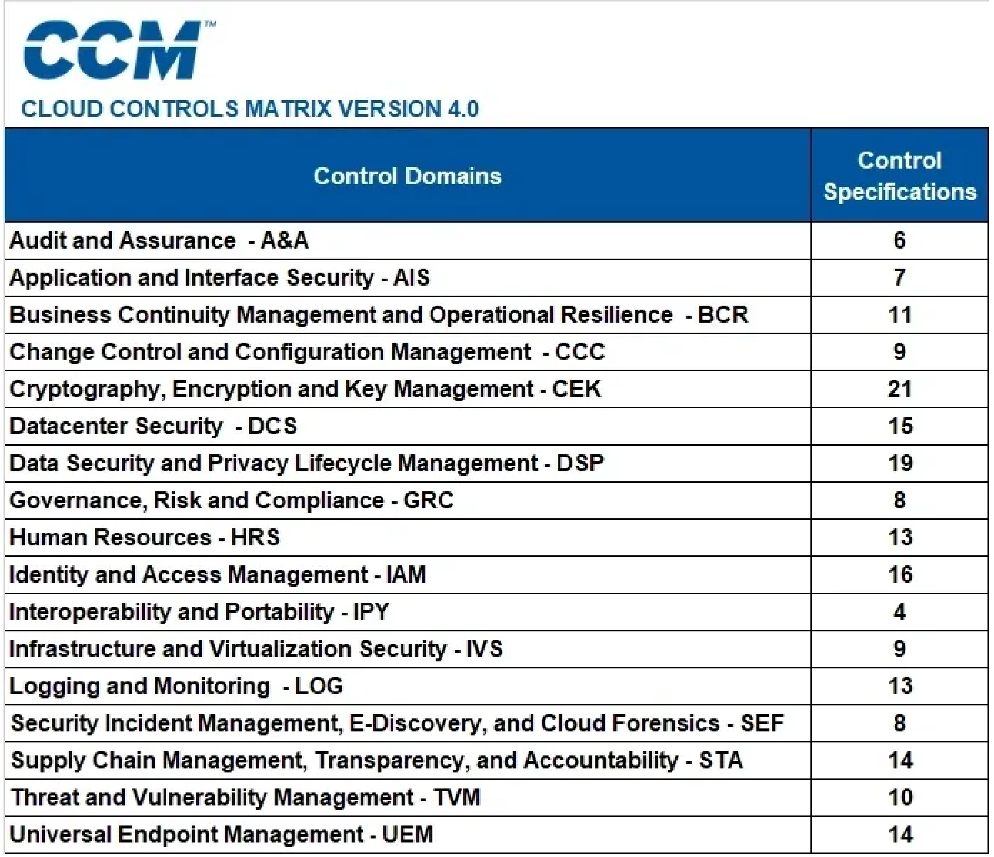
Born in 2008 and incorporated in 2009, the Cloud Security Alliance issued the first comprehensive best-practice document for secure cloud computing, “Security Guidance for Critical Areas of Focus for Cloud Computing,” and has become the industry body for frameworks, benchmarks, and standards associated with cloud computing worldwide. Some of the key documents developed include the Cloud Controls Matrix (CCM), the user credential Certificate of Cloud Security Knowledge (CCSK), the Certified Cloud Security Professional (CCSP) credential (developed jointly with ISC2), and a security framework for government clouds.

Regulations, Standards, and Frameworks

Key Frameworks

Cloud Security Alliance
Cloud Controls Matrix

The Cloud Controls Matrix (CCM) is a meta-framework of cloud-specific security controls, mapped to leading standards, best practices, and regulations. This document uses 16 domains to cover 133 security control objectives to address all key aspects of cloud security. The controls document are mapped to the main industry security standards, including ISO 2700X series, NIST SP 800-53, PCI DSS, ISACA COBIT, and many others



CCM™
CLOUD CONTROLS MATRIX VERSION 4.0

Control Domains	Control Specifications
Audit and Assurance - A&A	6
Application and Interface Security - AIS	7
Business Continuity Management and Operational Resilience - BCR	11
Change Control and Configuration Management - CCC	9
Cryptography, Encryption and Key Management - CEK	21
Datacenter Security - DCS	15
Data Security and Privacy Lifecycle Management - DSP	19
Governance, Risk and Compliance - GRC	8
Human Resources - HRS	13
Identity and Access Management - IAM	16
Interoperability and Portability - IPY	4
Infrastructure and Virtualization Security - IVS	9
Logging and Monitoring - LOG	13
Security Incident Management, E-Discovery, and Cloud Forensics - SEF	8
Supply Chain Management, Transparency, and Accountability - STA	14
Threat and Vulnerability Management - TVM	10
Universal Endpoint Management - UEM	14

Regulations, Standards, and Frameworks

Benchmarks and Secure Configuration Guides

Benchmarks and secure configuration guides offer guidance for setting up and operating computer systems to a secure level that is understood and documented. As each organization may differ, the standard for a benchmark is a consensus-based set of knowledge designed to deliver a reasonable set of security across as wide a base as possible

Center for Internet Security (CIS) benchmarks

National Checklist Program (NCP)

Security Technical Implementation Guides (STIGs).

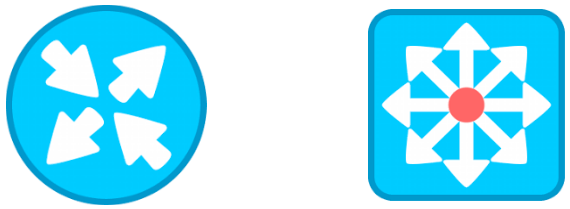
Regulations, Standards, and Frameworks

Benchmarks and Secure Configuration Guides

Platform/Vendor-Specific Guides

Web Server

OS



Network Devices

Organizational Policies

Organizational Policies

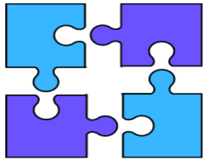
This chapter covers CompTIA Security+ exam objective 5.3:
Explain the importance of policies to organizational security

Personnel Policy

AUP

Job Rotation Policy

Mandatory Vacation



Separation of Duties

Least Privilege

Organizational Policies

Personnel Policy

Clean Desk Space

Background Checks

Non Disclosure Agreement

Onboarding

Off boarding

Organizational Policies

User Training

Gamification

Capture the Flag

Phishing Campaigns

Computer-Based Training (CBT)

Organizational Policies

User Training

Role-Based Training

Diversity of Training Techniques

Organizational Policies

Third-Party Risk Management

Service Level Agreement (SLA)

Memorandum of Understanding

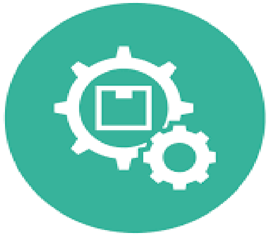
Measurement Systems Analysis

Organizational Policies

Third-Party Risk Management

Business Partnership Agreement

End of Life

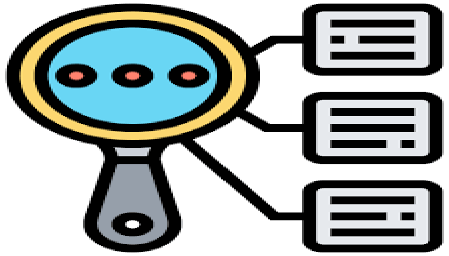


End of Service Life (EOSL)

Organizational Policies

Third-Party Risk Management

Data



Data Classification

Data Governance

Data Retention

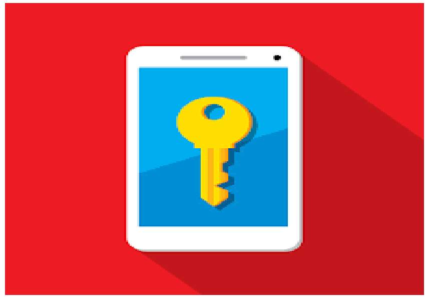
Organizational Policies

Credential Policies

Credential policies refer to the processes, services, and software used to store, manage, and log the use of user credentials. User-based credential management solutions are typically aimed at assisting end users in managing their growing set of passwords.

Personnel

Third Party



Devices

Service Accounts

Administrator/Root Accounts

Organizational Policies

Organizational Policies

Change Management

Change control

Asset Management

Risk Management

Risk Management

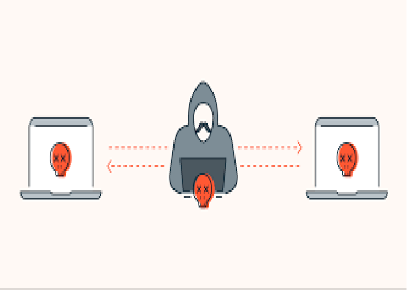
This chapter covers CompTIA Security+ exam objective 5.4:
Summarize risk management processes and concepts.

Risk Types

External Threat

Internal

Legacy Systems



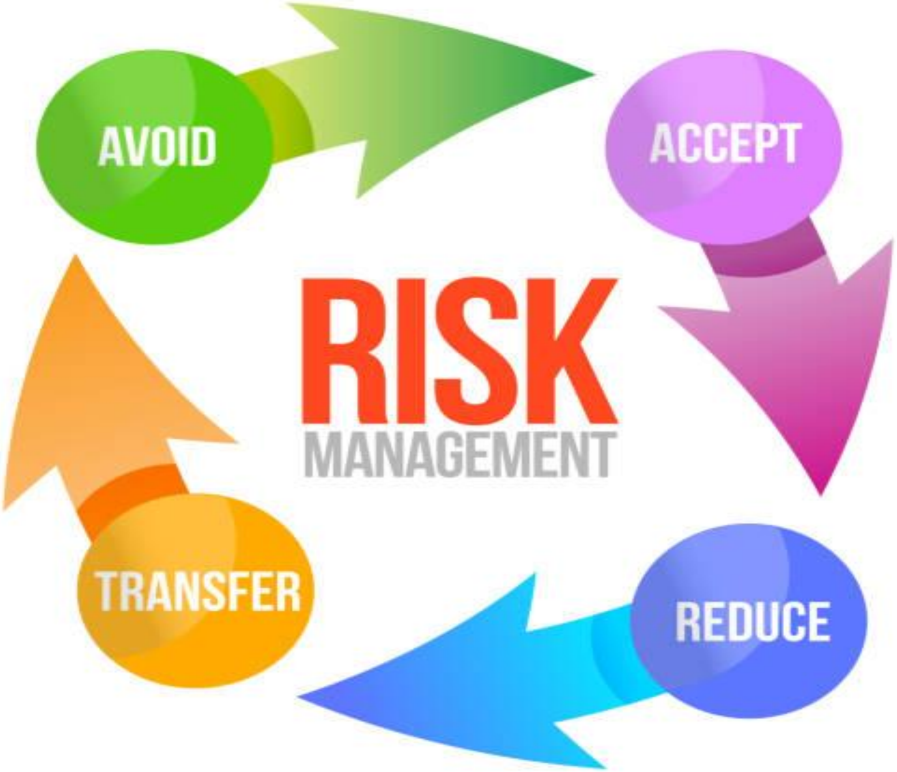
IP Theft

Software Compliance/Licensing

Risk Management

Risk Management Strategies

Risk management can best be described as a decision-making process. Risk management strategies include elements of threat assessment, risk assessment, and security implementation concepts



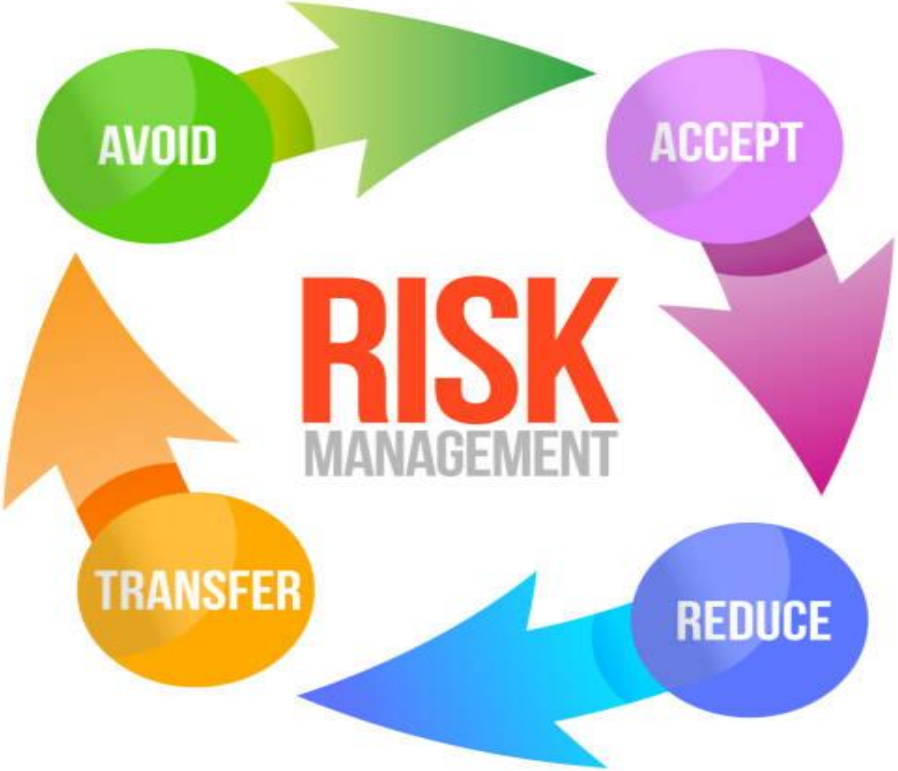
Risk Management

Acceptance

When you're analyzing a specific risk, after weighing the cost to avoid, transfer, or mitigate a risk against the probability of its occurrence and its potential impact, the best response is to accept the risk. For example, a manager may choose to allow a programmer to make "emergency" changes to a production system (in violation of good separation of duties) because the system cannot go down during a given period of time

Avoidance

Risk avoidance is the elimination of hazards, activities and exposures that can negatively affect an organization and its assets.



Risk Management

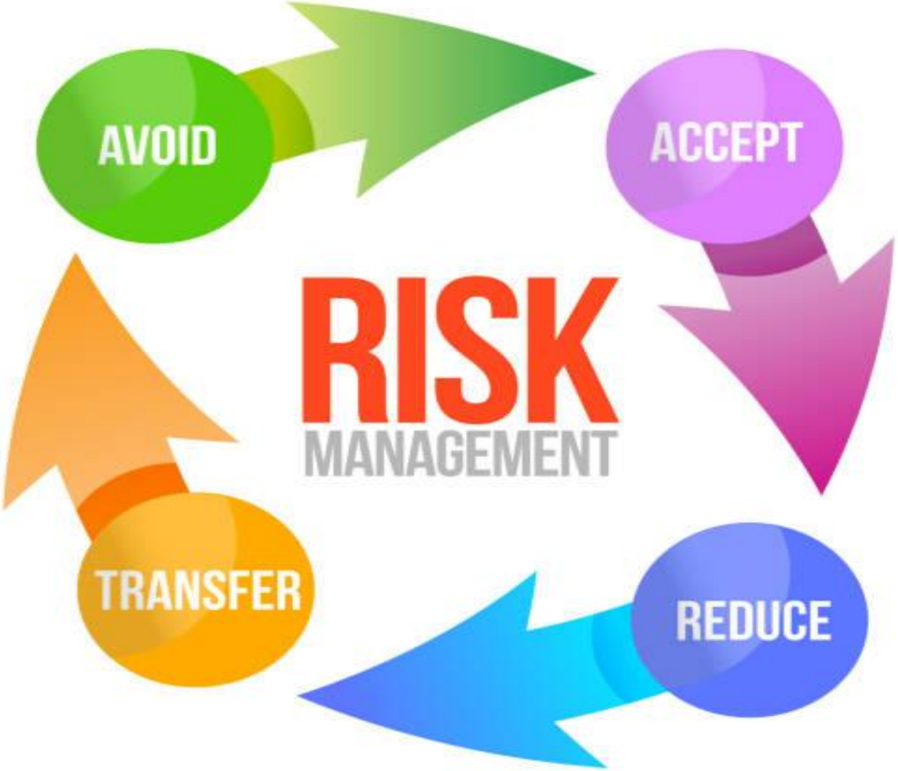
Transference

Transference of risk is when the risk in a situation is covered by another entity. As mentioned previously surrounding issues such as cloud computing, contracts and legal agreements will denote which parties are assuming which risks.

Cybersecurity Insurance a common method of transferring risk is to purchase cybersecurity insurance. Insurance allows risk to be transferred to a third party that manages specific types of risk for multiple parties, thus reducing the individual cost.

Mitigation

Risk can also be mitigated through the application of controls that reduce the impact of an attack. Controls can alert operators so that the level of exposure is reduced through process intervention.



Risk Management

Risk Analysis

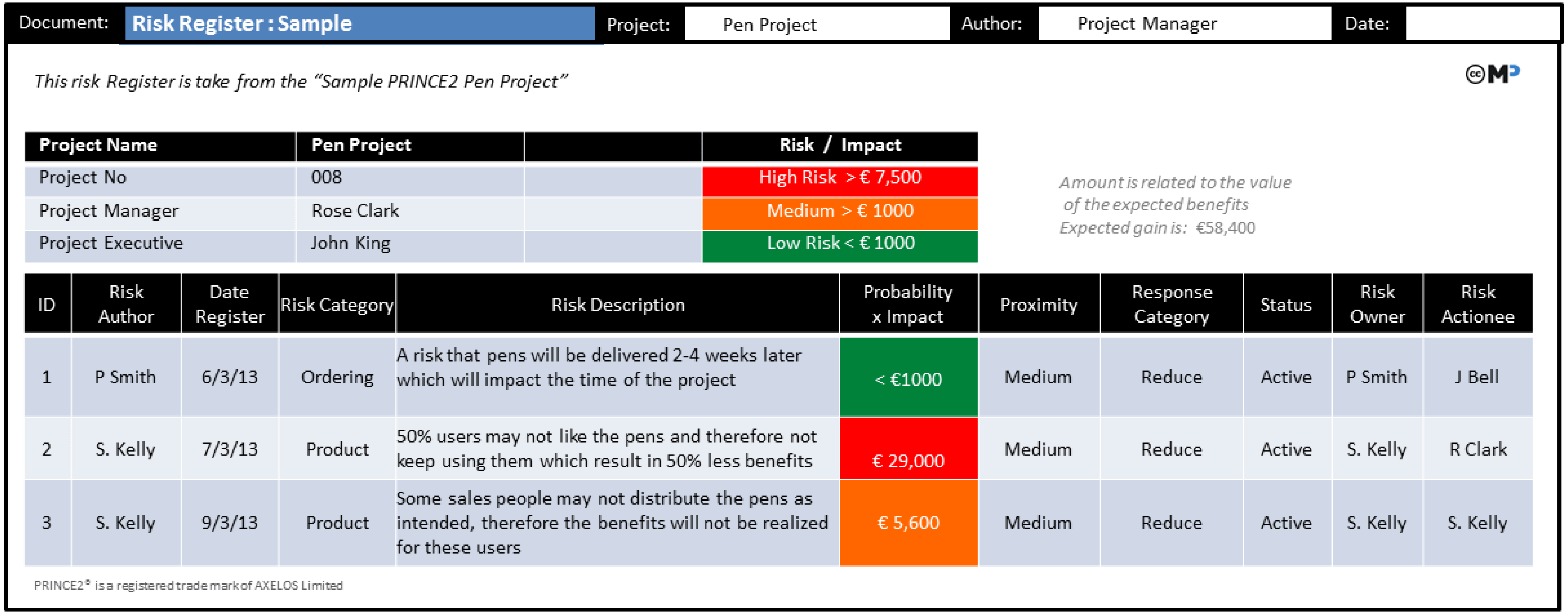
To effectively manage anything, there must be appropriate measurements to guide the course of actions. In the case of risk, this is also true. To manage risk, there needs to be a measurement of loss, and potential loss, and much of this information comes by way of risk analysis. Risk analysis is performed via a series of specific exercises that reveal presence and level of risk across an enterprise. Then, through further analysis, the information can be refined to a workable plan to manage the risk to an acceptable level.

Risk Analysis
Identify All Risks + Risk Assessment +Positive Action to Control it

Risk Management

Risk Register

A risk register is a list of the risks associated with a system. It also can contain additional information associated with the risk element, such as categories to group like risks, probability of occurrence, impact to the organization, mitigation factors, and other data.



Document:	**Risk Register : Sample**	Project:	Pen Project	Author:	Project Manager	Date:	

This risk Register is take from the "Sample PRINCE2 Pen Project"

Project Name	Pen Project		Risk / Impact
Project No	008		High Risk > € 7,500
Project Manager	Rose Clark		Medium > € 1000
Project Executive	John King		Low Risk < € 1000

Amount is related to the value of the expected benefits
Expected gain is: €58,400

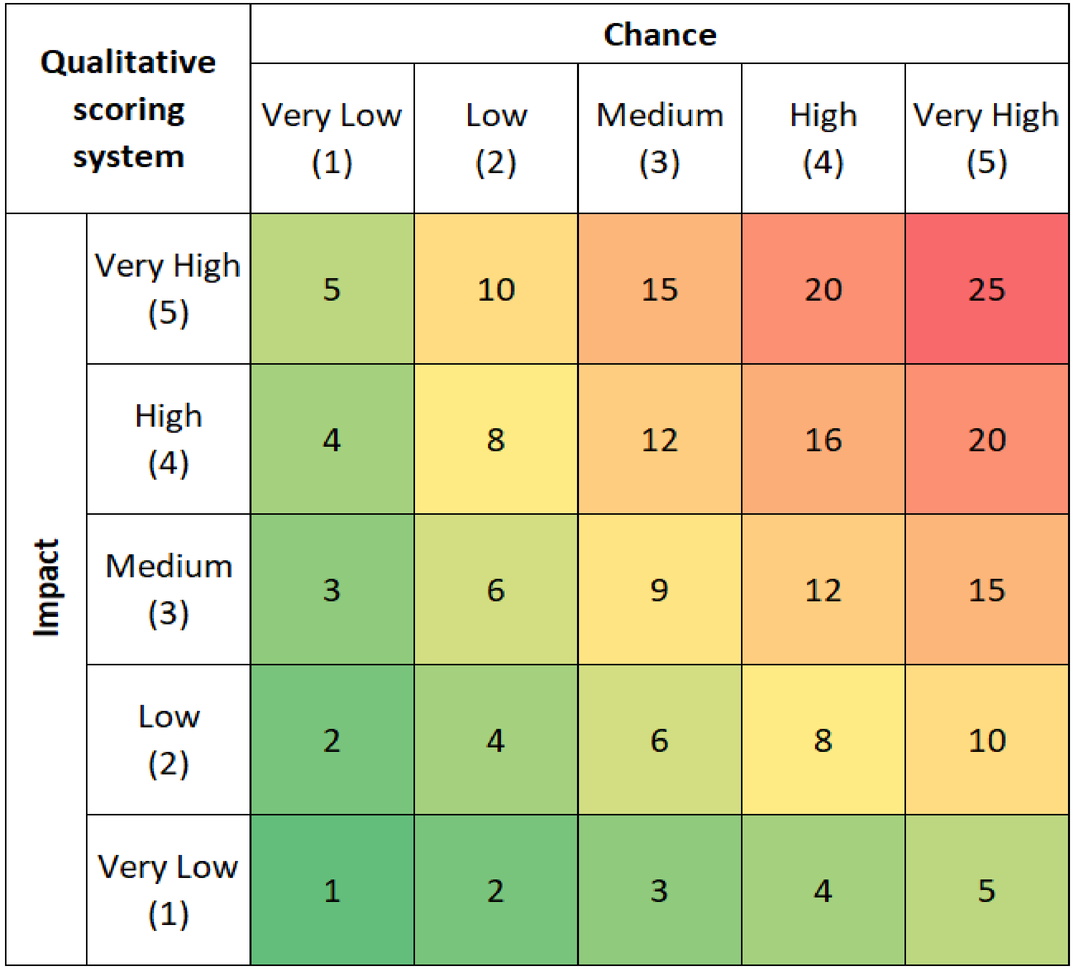
ID	Risk Author	Date Register	Risk Category	Risk Description	Probability x Impact	Proximity	Response Category	Status	Risk Owner	Risk Actionee
1	P Smith	6/3/13	Ordering	A risk that pens will be delivered 2-4 weeks later which will impact the time of the project	< €1000	Medium	Reduce	Active	P Smith	J Bell
2	S. Kelly	7/3/13	Product	50% users may not like the pens and therefore not keep using them which result in 50% less benefits	€ 29,000	Medium	Reduce	Active	S. Kelly	R Clark
3	S. Kelly	9/3/13	Product	Some sales people may not distribute the pens as intended, therefore the benefits will not be realized for these users	€ 5,600	Medium	Reduce	Active	S. Kelly	S. Kelly

PRINCE2® is a registered trade mark of AXELOS Limited

Risk Management

Risk Matrix/Heat Map

A risk matrix or heat map is used to visually display the results of a qualitative risk analysis. This method allows expert judgment and experience to assume a prominent role in the risk assessment process and is easier than trying to exactly define a number for each element of risk. To assess risk qualitatively, you first determine the likelihood of a threat occurring and also the consequence should it occur. You then take the value of each and multiply them together to get the risk value

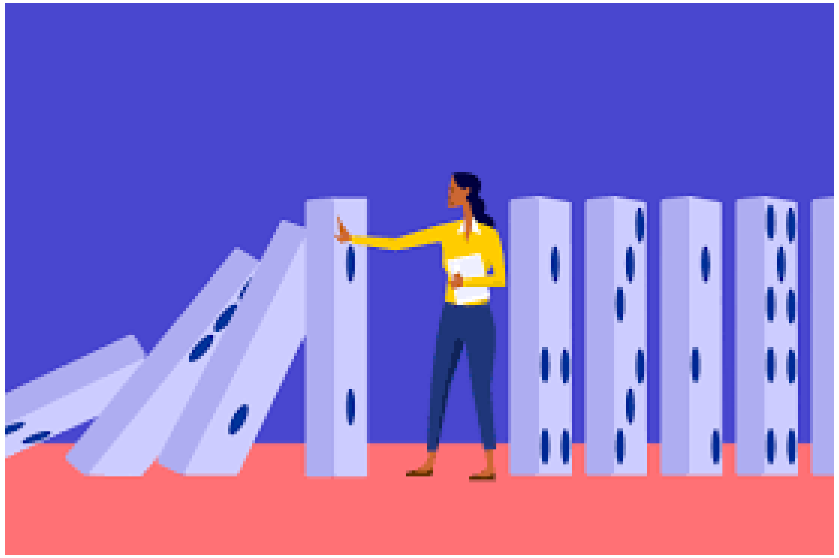


Qualitative scoring system		Chance				
		Very Low (1)	Low (2)	Medium (3)	High (4)	Very High (5)
Impact	Very High (5)	5	10	15	20	25
	High (4)	4	8	12	16	20
	Medium (3)	3	6	9	12	15
	Low (2)	2	4	6	8	10
	Very Low (1)	1	2	3	4	5

Risk Management

Risk Awareness

Risk awareness is knowledge of risk and consequences. Risk awareness is essential for wide ranges of personnel, with the content tailored to their contributions to the enterprise. For some workers, understanding the risks and defenses against social engineering is important. For others, such as designers of systems, more detailed understanding of risk and the vulnerabilities that cause it are needed. For management and executives, an understanding of the whole risk ecosystem is necessary because they must balance the risk and reward through major system initiatives.



Risk Management

Inherent Risk

All organizations in all industries face a certain amount of inherent risk. Inherent risk is the amount of risk that exists when some threat goes untreated or unaddressed. This also means that the less an organization tries to manage risk, the more inherent risk it has.

Residual Risk

The presence of risks in a system is an absolute—they cannot be removed or eliminated. As mentioned previously in this chapter, four actions can be taken to respond to risk: accept, transfer, avoid, and mitigate. Whatever risk is not transferred, mitigated, or avoided is referred to as residual risk and, by definition, is accepted.

Risk Management

Control Risk

Control risk is the probability that financial statements are materially misstated, due to failures in the controls used by a business. When there are significant control failures, a business is more likely to experience undocumented asset losses, which mean that its financial statements may reveal a profit when there is actually a loss.

Risk appetite

Is the term used to describe a firm's tolerance for risk. Even within a sector, with companies of the same size, operating in roughly the same areas, there can be differences in the level of risk each feels comfortable in accepting. This risk appetite is related to other business elements such as reward and loss. Each company's executive structure needs to determine the appropriate risk appetite for that firm, and that becomes the upper limit on acceptable risk in the company's operations.

Risk Management

Risk Assessment Types

Qualitative risk assessment is the process of subjectively determining the impact of an event that affects a project, program, or business. Qualitative risk assessment usually involves the use of expert judgment and models to complete the assessment.

Quantitative risk assessment is the process of objectively determining the impact of an event that affects a project, program, or business. Quantitative risk assessment usually involves the use of metrics and models to complete the assessment. Quantitative risk assessment applies historical information and trends to attempt to predict future performance..

Qualitative Analysis
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.
Subjective Evaluation
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.
Quantitative Analysis
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.
Numerical Evaluation
This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

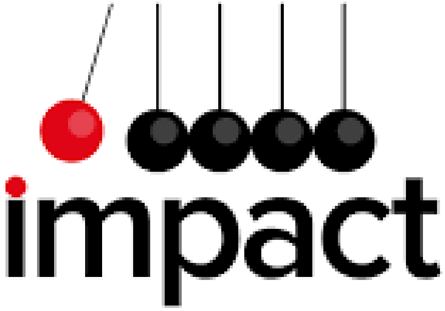
Risk Management

Likelihood of Occurrence

The likelihood of occurrence is the chance that a particular risk will occur. This measure can be qualitative or quantitative, as just discussed.

Impact

The impact of an event is a measure of the actual loss when a threat exploits a vulnerability. Federal Information Processing Standard (FIPS) 199 defines three levels of impact using the terms high, moderate, and low. The impact needs to be defined in terms of the context of each organization, as what is high for some firms may be low for much larger firms.



Risk Management

Impact

Injury and loss of life

Property

Safety

Finance

Risk Management

Asset Value

The asset value (AV) is the amount of money it would take to replace an asset. This term is used with the exposure factor (EF), a measure of how much of an asset is at risk, to determine the single-loss expectancy (SLE).

Single-Loss Expectancy (SLE)

The single-loss expectancy (SLE) is the value of a loss expected from a single event. It is calculated using the following formula: SLE = asset value (AV) × exposure factor (EF)

Exposure factor (EF) is a measure of the magnitude of loss of an asset. For example, to calculate the exposure factor, assume the asset value of a small office building and its contents is $2 million. Also assume that this building houses the call center for a business, and the complete loss of the center would take away about half of the capability of the company. Therefore, the exposure factor is 50 percent, and the SLE is calculated as follows:

SLE= $2 million × 0.5 = $1 million

Risk Management

Annualized Loss Expectancy (ALE)

After the SLE has been calculated, the annual loss expectancy (ALE) is then calculated simply by multiplying the SLE by the likelihood or number of times the event is expected to occur in a year, which is called the annualized rate of occurrence (ARO):

ALE = SLE × ARO

Annualized Rate of Occurrence (ARO)

The annualized rate of occurrence (ARO) is a representation of the frequency of the event, measured in a standard year. If the event is expected to occur once in 20 years, then the ARO is 1/20.

ALE is $1 million × 1/20 = $50,000

Risk Management

Disasters

Disasters are major events that cause disruptions. The timescale of the disruption can vary, as can the level of disruption, but the commonality is that the external event that caused the disruption is one that cannot be prevented. Foreseen, yes, but prevented, not necessarily. Common disasters include weather-related events and events that everyone knows will happen eventually, just not where or when.

Environmental

One of the largest sources of threats is from the environment. Environmental changes can come from a wide variety of sources—weather, lightning, storms, and these can cause changes to the system in a manner that disrupts normal operations. These changes can increase risk. While IT security measures cannot change the environmental factors that can impact operations, they can have an effect on the risk associated with the environmental issue. Making systems resilient can reduce impacts and mitigate these sources of risk to the enterprise.

Risk Management

Person-made

Person-made threats are those that are attributable to the actions of a person. But these threats aren't limited to hostile actions by an attacker; they include accidents by users and system administrators. Users can represent one of the greatest risks in an IT system. More files are lost by accidental user deletion than by hackers deleting files, and to the team trying to restore the lost files, the attribution has no bearing on the restoration effort.

Internal vs. External

As mentioned previously in the chapter, threats can come from internal and external sources. Internal threats have their origin within an organization, whereas external risks come from the outside. When disasters are examined, they can be seen to have originated either within the company or outside the company. While it is easy to always blame an outside force, in many cases, internal policies and procedures increase a firm's risk profile for easily understood external risks.

Risk Management

Business Impact Analysis

Business impact analysis (BIA) is the process used to determine the sources and relative impact values of risk elements in a process. It is also the name often used to describe a document created by addressing the questions associated with sources of risk and the steps taken to mitigate them in the enterprise. The BIA also outlines how the loss of any of your critical functions will impact the organization.

© CanStockPhoto.com - csp97758447

Recovery Time Objective (RTO)

The term recovery time objective (RTO) is used to describe the target time that is set for the resumption of operations after an incident. This is a period of time that is defined by the business, based on the needs of the business. A shorter RTO results in higher costs because it requires greater coordination and resources. This term is commonly used in business continuity and disaster recovery operations

Risk Management

Functional Recovery Plans

Accidents, disasters, and interruptions to business processes happen. This is why we have business continuity plans (BCPs). But what comes next? Functional recovery plans represent the next step—the transition from operations under business continuity back to normal operations. Just as the transition to business continuity operations needs to be planned, so too does the functional recovery plan.

Single Point of Failure

A key principle of security is defense in depth. This layered approach to security is designed to eliminate any specific single point of failure (SPOF). A single point of failure is any system component whose failure or malfunctioning could result in the failure of the entire system. An example of a single point of failure would be a single connection to the Internet

Risk Management

Disaster Recovery Plan (DRP)

A disaster recovery plan (DRP) is the plan a firm creates to manage the business impact of a disaster and to recover from its impacts.

Mission-Essential Functions

When examining risk and impacts to a business, it is important to identify mission-essential functions from other business functions. In most businesses, the vast majority of daily functions, although important, are not mission essential. Mission-essential functions are those that, should they not occur or be performed properly, will directly affect the mission of the organization.

Risk Management

Identification of Critical Systems

A part of identifying mission-essential functions is identifying the systems and data that support the functions. Identification of critical systems enables the security team to properly prioritize defenses to protect the systems and data in a manner commensurate with the associated risk

Site Risk Assessment

Risk assessments can have specific characteristics associated with different sites. This is the basis for a site risk assessment, which is simply a risk assessment tailored for a specific site. In organizations with multiple locations, with differing systems and operations, having tailored risk assessments that are specific to the risks associated with each site provides information for the firm.

Core Financial Management

Privacy

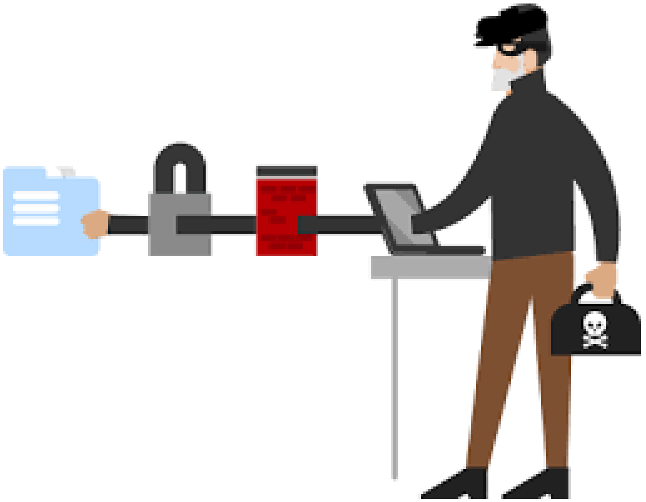
Privacy

Organizational Consequences of Privacy breaches

When a company loses data that it has stored on its network, the term used is data breach. Data breaches have become an almost daily news item, and the result is that people are becoming desensitized to their occurrence. Data breaches act as a means of notification that security efforts have failed

Reputation Damage

Reputation damage is a form of damage against a firm’s brand. Customers exert a choice when they engage in a commerce transaction, and businesses spend a lot of time and resources on building brands that facilitate the purchase decision towards their firm. Having to notify all customers of a breach/disclosure event is truly damaging to a firm’s brands.



Privacy

Identity Theft

Identity theft occurs when a criminal, using stolen information, assumes the identity of another individual to obtain and use credit in the victim's name. If the data disclosure results in loss of customer personal information.

Fines

Regulatory agencies, such as the Federal Trade Commission (FTC), have the ability to levy fines when regulations are not followed. These fines are not minor. In the EU, General Data Protection Regulation (GDPR) fines can be 4% of a firm's revenue, and fines in the hundreds of millions of euros have been levied

Privacy

Notifications of Breaches

In an ideal world, there would never be any data breaches, so there would never be a need for processes in the event of data breaches. But it is not an ideal world, and breaches do happen. And even if one hasn't happened to your firm yet, virtually every government jurisdiction has enacted a series of laws and regulations covering a firm's responsibilities in the event of a breach. Understanding and being prepared to issue notifications of breaches in accordance with these laws and directives is important, because once a breach occurs, the timelines to do the correct things are short and the penalties can be significant

Escalation

When a data breach occurs in the enterprise, it is important to have a process for escalating the incident up through your organization. Most data breaches are discovered as part of some incident response process, and the breach needs to have its own response separate from the initiating incident. Establishing a breach escalation policy, with the accompanying procedures, will ensure proper levels of management attention to this critical process.

Privacy

Public Notifications and Disclosures

Many laws and regulations covering information breaches require public disclosure of computer security breaches in which unencrypted confidential information of any resident may have been compromised. These laws apply to any person or entity that does business in the regulated jurisdiction, even if located out of state, and that owns or licenses computerized data that includes personal information.

Privacy

Classifications

Public data is data that can be seen by the public and has no needed protections with respect to confidentiality. It is important to protect the integrity of public data, lest one communicate incorrect data as being true

Private Data is labeled private if its disclosure to an unauthorized party would potentially cause harm or disruption to the organization. Passwords could be considered private.

Sensitive data is a generalized term that typically represents data classified as restricted from general or public release. This term is often used interchangeably with confidential data.

Confidential data is labeled confidential if its disclosure to an unauthorized party would potentially cause serious harm to the organization. Such as customer data, internal business plans

Critical Data is labeled critical if its disclosure to an unauthorized party would potentially cause extreme harm to the organization, such as trade secrets, proprietary software code, and new product designs

Privacy

Classifications

Public data is data that can be seen by the public and has no needed protections with respect to confidentiality. It is important to protect the integrity of public data, lest one communicate incorrect data as being true

Private Data is labeled private if its disclosure to an unauthorized party would potentially cause harm or disruption to the organization. Passwords could be considered private.

Sensitive data is a generalized term that typically represents data classified as restricted from general or public release. This term is often used interchangeably with confidential data.

Confidential data is labeled confidential if its disclosure to an unauthorized party would potentially cause serious harm to the organization. Such as customer data, internal business plans

Critical Data is labeled critical if its disclosure to an unauthorized party would potentially cause extreme harm to the organization, such as trade secrets, proprietary software code, and new product designs